

Business Continuity For Small and Medium-Sized Firms

AL BERMAN, RISK SOLUTIONS INTERNATIONAL LLC



THE NEED FOR BUSINESS CONTINUITY PLANNING has grown rapidly in the 21st century, driven by both regulatory compliance requirements and customer demands. Business continuity is as critical to small and medium-sized companies as it is to their larger competitors. Small (defined here as having annual revenue of less than \$25 million) and medium-sized businesses (annual revenue of less than \$200 million), however, often have limited financial resources and expertise to spend on planning to keep operations going during a crisis.

Smaller business owners have a tendency to rely upon their instincts as “smart people” to solve what may appear to be a simple problem—a mistake that almost inevitably results in an ineffective business continuity plan (BCP). A far better approach is to consider business continuity as part of an overall risk transfer program. Risk transfer is defined as mitigating risk, using insurance to offset loss, and transferring obligations to other entities. A risk transfer program includes risk assessment and mitigation as well as insurance coverage. The planning process establishes good business practices that add operational resilience and reliability in manufacturing, services, and distribution industries in both the public and private sectors. Business continuity, which was once a “nice to have” feature, has become mandatory to maintain customer confidence and a competitive edge in these days of uncertainty.

One need only look at the effort being expended by corporations to realize how important business continuity has become in marketing—a direct reflection of the concerns of the regulators and customers. Web sites have begun to add links to business continuity programs; customer mailings include flyers that detail a company’s continuity efforts and reinforce the message that during a crisis, “We’ll be here for you.” Marketing business continuity is beginning to rival preparing for Y2K.

Recent events, both large and small, have added a sense of urgency to guaranteeing that a business is up to the task of delivering goods and services while it is operating under

duress, and we have seen the consequences of not being prepared:

- A lightning bolt sets fire to a chip manufacturing plant and the mobile phone industry sees a major shift in the competitive landscape.
- A major drug manufacturing plant fails an FDA inspection and negatively impacts its financial picture.
- Docks on the West Coast are closed as a result of a union action, sharply curtailing the production and delivery of goods and causing severe adverse revenue and profit impacts downstream.
- Hurricanes in the South disrupt agriculture and manufacturing production, as well as the delivery of goods and materials.

During any type of crisis, a company’s BCP must maintain the viability of the business process and maintain a previously agreed-upon level of service as defined by the appropriate authority of an organization. This level can be determined through a business impact analysis (BIA) or some other means that complies with informed business judgment, regardless of the size of the business entity. Loss of facility, interruption of the business process, or disruption of IT capabilities and/or telephony will decrease operating capabilities. The challenge facing small and medium-sized businesses is how to construct a BCP that will help them survive in a competitive landscape that demands reliability and resilience.

The Requirement

Regulatory requirements for business continuity, particularly in the financial and healthcare arenas, have far-reaching effects that extend beyond the organizations falling under the jurisdiction of the regulatory body into companies that are third-party providers, key suppliers, and business partners. The regulatory language suggests that companies review plans and test results of those who they deem vital to their operational process. There is even a recommendation made by the Federal Financial Institution Examination Council (FFIEC)

that these other parties actively participate in testing the BCP.

Even organizations not covered by specific regulatory mandates have taken a proactive approach to ensuring that their suppliers will not cause them to fail to produce and deliver products to their end customers in the event of a crisis. Vendor continuity management has become a concern, and in some cases a directive, to all suppliers, distributors, vendors, and third-party business partners. One major electronics firm has issued an edict to all its suppliers, regardless of size, directing them to have a BCP and to provide test results that prove compliance. Failing to comply can result in the end of supplier's business relationship with the firm. And the U.S. Department of Defense has gone so far as to require an independent review of testing procedures to increase its level of confidence.

Business continuity will inevitably become a cost of doing business for all companies. Size will not matter, although some government regulations—most notably HIPAA (Health Insurance Portability and Accountability Act), have granted extra time for “small” entities to comply. Companies small, medium, and large will have to ensure the regulators or their customers that they will be able to provide goods, services, and distribution in the event that they are affected by a disaster.

The Challenge

Small and medium-sized companies suffer two distinct disadvantages when providing effective continuity of operations and recovery. The first is that a smaller company often feels the impact of a particular crisis harder than a larger company. A large company, for example, can offset the effect of a hurricane in Florida that destroyed a distribution center by switching delivery and distribution to another center. A smaller entity that operates with a single site, however, will suffer greater short- and long-term losses. The short-term loss will result from losing stored goods and being unable to deliver goods in the days immediately following the incident. In the long-term, not being able to deliver goods in the ensuing weeks or even months will translate into lost market share. And because it is likely that the company's technology is located at the affected site, a disaster will also severely curtail the ability to maintain vital IT processing. Service organizations located in a single site will suffer a similar fate.

The second disadvantage that small and medium firms have is that they are limited in terms of personnel and budget. With the exception of financial institutions, few small or medium-sized companies have direct BCP experience, that is, not obtained through hired consultants. Most smaller companies do not have personnel dedicated to BCP, and few have a budget for the effort.

As more and more companies have discovered over the last few years, cost-effective and operationally sound business continuity planning demands the knowledge those who are professionally trained and experienced. “Smart people working hard” is not enough to create a sound and actionable

program. Most small and medium-sized firms find it difficult to support a BCP and often draft someone from human resources, facilities, security, finance, audit, legal, or IT to become the business continuity coordinator. Surveys by companies such as tax and advisory firm KPMG indicate that the larger a company is, the more dedicated BCP personnel it tends to employ. Smaller organizations may think that dedicated BCP is a luxury, but untrained and ill-equipped personnel tend to make mistakes that a seasoned practitioner would not.

A new business continuity coordinator is often struck by the lack of budget to acquire needed facilities, equipment, and technology. Yet they are faced with the challenge of developing an actionable BCP to carry a company through a crisis and save the day by allowing it to stay in business. The coordinator may also find that there is no staff to support continuity planning efforts. Department personnel whose input and time are required are too busy with day-to-day activities to provide information and guidance. And of course, a BCP is usually expected to be developed in addition to one's “day job.”

In the past, small and medium-sized firms would often develop a BCP based on hastily prepared documents, using off-the-shelf software to prepare a document to be stored away in red binders, ready to be examined by auditors, regulators, or clients. This may have been a viable strategy then, but today auditors, clients, and regulators have grown more knowledgeable and sophisticated. Armed with detailed regulatory and best-practice checklists, they are rejecting hastily prepared, ambiguous BCPs and are becoming more vigilant in their demands. Once roused by a less-than-adequate plan, reexaminations become more frequent and more stringent. More importantly, in a true emergency an inadequate BCP will not do what is intended to do—maintain a predetermined level of business operations.

The Plan

When developing a BCP, conducting a BIA is the best way to understand the issues confronting your organization. In addition to the business owners, enlist the aid of your risk manager, insurance broker, or insurance agent. Developing a full risk transfer model (of which BCP is a part) requires the participation of insurance professionals—cyber insurance, business interruption insurance, contingent business interruption, and extra expense insurance—who understand losses and coverage that will result from an outage to your business operations, especially in the event of physical damage.

It is important to predict the financial and qualitative losses that will be incurred at a given point in time (hours, days, weeks) after a business interruption in order to prevent irreparable damage the organization. Analyze current capabilities in terms of resources—where the company might relocate during an emergency and the capacity of the relocation site; how quickly it will be able to recover business and technology

Small and Medium Firms

(including voice and data communications); and finally, how much data will be lost if the IT facility is down. By comparing a business's needs to its capabilities, it is possible to develop an effective strategy to fill the gaps that will need to be closed in the event of a business interruption. An effective BCP is not simply an issue of financial impact, because regulatory bodies do not care whether an enterprise can afford to comply or not. Business continuity is simply a cost of doing business.

After the gaps that will need to be filled have been identified, it is time to create a cost-effective strategy to do so. A company that operates with multiple sites can create a strategy to shift the workload, the communications services, and the business technology to another site. An organization that has a single site may try to enlist the assistance of business associates and vendors. For example, when a primary government dealer was forced to leave the World Trade Center after the bombing in 1993, it was "taken in" by a large institutional dealer and was able to continue critical operations. After September 11, many displaced companies were housed in offices of their auditors and insurance brokers. Outside counsel, insurance brokers, bankers, etc. may be willing to provide a client with temporary office space in an emergency on a *best effort basis*, which means a willingness to provide help without implying a contractual relationship or liability. Equipment suppliers may be another source of emergency operational sites.

Contractors, commercial sites, and even competitors can coordinate a strategy that allows manufacturers and distributors to maintain long-term market share at the expense of short-term profits during a crisis. Before selecting a strategy, examine your extra expense insurance to understand at what point the company will be reimbursed for expenses associated with recovering and operating your business. Some policies begin compensation only after a certain amount of time, usually 24 to 48 hours.

Never underestimate the impact of losing of vital information and data (vital records) as the result of an outage. Critical data should be backed up at least once a day and stored offsite. The inability to reconstruct critical information will result in the loss of customer, order, financial, production, personnel, and supplier information that impair the ability to make business decisions, provide customer service, and maintain sound fiscal management.

Do not limit backups to only electronic information. The loss of paper records can also cause problems, ranging from inconvenience to considerable harm. Not having duplicate

personnel records that substantiate performance appraisals, reprimands, etc., for example, leave a company vulnerable to personnel actions. Not having access to beneficiary forms will severely impact processing claims at a time when anxiety is high and patience is in short supply. Copies of many other documents, from corporate charters to research notebooks, should be kept offsite to reduce the impact created by their loss. Determine which of the company's records are considered vital during the BIA.

Testing and Maintenance

The validity of an organization's BCP must be ensured through regular tests as defined by regulators—FFIEC, HIPAA, Federal Energy Regulatory Commission, etc. But a test should be conducted at least once a year, even when not dictated by regulatory mandate. Testing should entail reviews of roles and responsibilities, notification and activation procedures, and at minimum, a walk-through of recovery tasks. A tabletop exercise with all involved parties can meet the "test" threshold if it is interactive and requires outside parties to participate.

Finally, ensure that you have a process by which plans can be distributed and maintained. CDs and USB removable disks are inexpensive and easy to transport and install on almost any PC at recovery sites, at home, and on rental machines. While Web-based databases are critical, they are not easily transportable during an emergency. Large binders are ineffective and are seldom maintained, but plan summaries and wallet cards of important information should be carried at all times by appropriate personnel.

Conclusion

A business entity's size is becoming less of a factor in the necessity to create, test, and maintain business continuity plans. Firms small, medium, and large are being mandated (by statute and/or client) to ensure business continuity. By taking a holistic risk transfer approach that analyzes needs and creates cost-effective strategies to meet those needs, small and medium-sized firms will be able to continue operations under adverse conditions. **CI**

Al Berman is an executive vice president and head of operational risk consulting at Risk Solutions International. Berman is a former CEO and CIO and has been performing BCP and emergency response services for over 15 years. He is a former National Practice Leader for two major management consulting firms. He can be contacted at (212) 842-1588 or at aberman@rsi-llc.com.

The Clear Choice



We're the *Business* in Business Continuity.

Management Conference 2005
CONTINUITY
insights

SHERATON NEW ORLEANS
MAY 16-18, 2005

www.continuityinsights.com

Strategies to Assure Integrity, Availability and Security

CONTINUITY *insights*

The Clear Choice



We're the *Business* in Business Continuity.

Management Conference 2005
CONTINUITY
insights

SHERATON NEW ORLEANS
MAY 16-18, 2005